**АННОТАЦИЯ**

В пояснительной записке представлен курсовой проект на тему: «Подсистема защиты для АС «Отдел кадров»».

Данная подсистема должна обеспечивать: разграничение и управление доступом, регистрацию и учёт пользователей системы и их действий, обеспечение целостности данных.

Пояснительная записка состоит из девяти разделов в соответствии с которыми спроектирована, и разработана данная подсистема защиты.

Также в пояснительной записке содержится описание объекта автоматизации, требования к компонентам системы, алгоритм работы системы, инструкция по эксплуатации системы, визуальные формы программных компонентов, таблицы, обработчики программных компонентов, объекты, используемые в системе.

Содержание

[1. ВВЕДЕНИЕ 6](#_Toc436754427)

[2. Назначение и цели создаНИЯ СИСТЕМЫ 8](#_Toc436754428)

[3. АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ 10](#_Toc436754429)

[4. ОПИСАНИЕ ПОСТАНОВКИ ЗАДАЧИ 14](#_Toc436754430)

[4.1 Подсистема контроля доступа 14](#_Toc436754431)

[4.2 Подсистема регистрации и учета 15](#_Toc436754432)

[4.3 Подсистема целостности 15](#_Toc436754433)

[5 АНАЛИЗ МЕТОДОВ РЕШЕНИЯ 17](#_Toc436754434)

[5.1 Методы и средства защиты информации 17](#_Toc436754435)

[5.2 Средства вычислительной техники защиты от НСД к информации 20](#_Toc436754436)

[5.3 Обоснование выбора среды программирования 22](#_Toc436754437)

[6 ИНФОРМАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ 23](#_Toc436754438)

[6.1 Концептуальная модель 23](#_Toc436754439)

[6.2 Логическая модель 23](#_Toc436754440)

[6.3 Физическая модель 25](#_Toc436754441)

[7 РАЗРАБОТКА ПРОГРАММНО-ИНФОРМАЦИОННЫХ КОМПОНЕНТОВ СИСТЕМЫ 27](#_Toc436754442)

[7.1 Алгоритм программы 27](#_Toc436754443)

[7.2 Разработка пользовательского интерфейса 28](#_Toc436754444)

[7.3 Описание программных модуле 28](#_Toc436754445)

[7.4 Тестирование подсистем АИС 49](#_Toc436754446)

[7.4.1 Тестирование подсистемы управления доступом 49](#_Toc436754447)

[7.4.2 Тестирование подсистемы регистрации и учета 49](#_Toc436754448)

[8 ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ 50](#_Toc436754449)

[8.1 Инструкция для администратора 50](#_Toc436754450)

[8.2 Инструкция для пользователей 50](#_Toc436754451)

[8.2.1 Техника безопасности 51](#_Toc436754452)

[8.2.2 Требование безопасности во время работы 51](#_Toc436754453)

[8.2.3 Требование безопасности в аварийных ситуациях 52](#_Toc436754454)

[8.2.4 Требование к безопасности после окончания работы 52](#_Toc436754455)

[9. ЗАКЛЮЧЕНИЕ 53](#_Toc436754456)

[Список используемых источников 54](#_Toc436754457)

[Техническое задание 55](#_Toc436754458)

1. **ВВЕДЕНИЕ**

В наше время, которое называют веком информационных технологий, особое значение во всех сферах человеческой деятельности играет информация. Сейчас все большее внимание уделяется информированности о том или ином объекте, будь это крупная фирма или человек. Без полной информации практически невозможно решать серьезные задачи, добиваться реализации своей цели.

Обеспечение информационной безопасности является сегодня одним из основных требований к информационным системам. Причина этого - неразрывная связь информационных технологий и основных бизнес-процессов в любых организациях, будь то государственные службы, промышленные предприятия, финансовые структуры, операторы телекоммуникаций.

Безопасность в сфере информационных технологий — это комплекс мер, и она должна восприниматься как система. Компьютерная безопасность имеет различные аспекты, среди которых нельзя выделить более значимые или менее. Здесь важно все. Нельзя отказаться от какой-либо части этих мер, иначе система не будет работать.

Обеспечение внутренней информационной безопасности является не только российской, но и мировой проблемой. Если в первые годы внедрения корпоративных локальных сетей большой проблемой компаний был несанкционированный доступ к коммерческой информации путем внешнего взлома (хакерской атаки), то сегодня с этим научились справляться.

Отдел кадров – это место, куда стекается информация о рабочих предприятия. В отделе кадров содержится информация о людях, работающих на данном предприятии, которая составляет их персональные данные. Функциональная роль отдела кадров на предприятии очень велика по той причине, что именно в отделе кадров мы находим интересующую нас информацию о рабочих и по этой же причине мы должны обеспечить ее конфиденциальность т.е. ограничить доступ к ней посторонних лиц, а также контролировать доступ к ней.

Но контроль и разграничение доступа это еще не все также появляется задача обеспечения целостности информации для предотвращения и контроля преднамеренных и случайных изменений в информационной системе.

Таким образом в данной предметной области необходимо внедрить и обеспечить функционирование основных подсистем информационной безопасности, а именно таких как:

* подсистема идентификации и аутентификации пользователей в системе,
* реализовать разграничение доступа пользователей.
* подсистема регистрации событий (вход/выход в/из системы)
* обеспечить подсистему информационной целостности.

1. **Назначение и цели создаНИЯ СИСТЕМЫ**

Автоматизированная система представляет собой организационно техническую структуру, состоящую из взаимосвязанных компонентов:

1. Технических средств обработки и передачи данных, методов и алгоритмов обработки данных в виде соответствующего программного обеспечения, информация (баз данных) на различных носителях личного состава (пользователей) системы объединенных по организационно – структурному, тематическому или иным признакам для выполнения автоматизированной обработки информации целью решения задач управления.
2. Защита системы обработки информации обеспечения безопасности конфиденциальности и целостности обрабатываемой информации и поддерживать свою работоспособность в условиях воздействия на нее заданного воздействия на ней множества угроз.

Задачи необходимые для создания защищенной системы:

1. В ходе автоматизации процесса обработки конфиденциальной информации должны быть реализованы все аспекты этого процесса связанные с обеспечением безопасности информации.
2. Должно обеспечиваться противодействие угрозам безопасности при эксплуатации защищенной системы.
3. Должны быть реализованы необходимые требования, соответствующие стандартам информационной безопасности

Для разработки подсистемы безопасности, необходимо определить общие цели защиты информации, которые изложены в федеральном законе от 27.07.2006 N 149-ФЗ «Об информации, информатизации и защите информации» по которому целями защиты являются:

* предотвращение утечки, хищения, утраты, искажения, подделки информации;
* предотвращение угроз безопасности личности, общества, государства;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
* защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
* сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;
* обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

1. **АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ**

Основными предпосылками для исследования предметной области «Отдел кадров», является потребность в автоматизации работы инспектор отдела кадров – создание базы данных кадрового состава предприятия (организация добавления, модификации информации о работниках предприятия, должностные инструкции и назначения его должности и отдела для дальнейшей работы. Целью является решение вышеописанной проблемы и создание такого программного обеспечения, которое удовлетворит все потребности по передачи, хранению данных, тем самым достичь снижения финансовых и временных затрат.

Анализируя предметную область «Отдел кадров» можно установить, что инспектор отдела кадров вводит данные о сотруднике и о его табеле, сотрудник может просматривать правильность заполненных данных о себе, а администратор следит за целостностью информации в системе, также контролирует доступ в нее.

Субъектами данной автоматизированной системы являются:

1. Инспектор отдела кадров
2. Администратор
3. Сотрудники (инженер, оператор, бухгалтер)

Объектами данной автоматизированной системы являются:

1. Сотрудник
2. Табель
3. Должность
4. Отдел
5. Журнал событий
6. Таблица логинов паролей

АС «Отдел кадров» представляет собой сложную структуру данных, т.к. ведется учет заполняемых данных инспектором отдела кадров, чтобы в дальнейшем составлять их рабочий табель, а редактировать их. Следующие полномочия у пользователей системы такие:

* Администратор – введет учет за входом/выходом в/из системы, ведет отчетность по журналу входа-выхода, выдает и обновляет пароли пользователям, ведет учет контроля целостности в системе и ведет контроль безопасности в соответствии с политикой безопасности;
* Инспектор отдела кадров – заполняет записи о сотрудниках, заполняет и распечатывает рабочий табель, редактирует и обновляет информацию о сотруднике, а также выдает логин сотрудникам
* Сотрудник – просматривает и проверят свои персональные данные.

Таблица 1 – Таблица разграничения полномочий (ТРП)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Сотрудник | Табель | Должность | Отдел | Журнал учета | ТКП | ТРП |
| Инспектор отдела кадров | RW | RW | R | R | - | - | - |
| Администратор | - | - | - | - | RW | RW | RW |
| Сотрудник | - | - | - | - | - | - | - |

* «R» - чтение;
* «W» - редактирование;
* «-» - не имеет доступа.

Таблица 2 – Классификация информации

|  |  |  |  |
| --- | --- | --- | --- |
| Пользователь | Документ | Вид тайны | Ссылка на закон |
| Инспектор отдела кадров | Информация о сотрудниках, табель сотрудника | Персональные данные | Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" |

Продолжение таблицы 2

|  |  |  |  |
| --- | --- | --- | --- |
| Сотрудник | Информация о сотрудниках | Персональные данные | Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" |
| Администратор | Таблица кодов и паролей, журнал учета | Персональные данные, служебная тайна | Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных"; Постановление ГД ФС РФ от 02.11.2011 N 6152-5 ГД "О проекте Федерального закона N 124871-4 "О служебной тайне" |

Для данной АС можно вывести следующие угрозы безопасности:

1. Разглашение, несанкционированная модификация, подмена или уничтожение конфиденциальной информации, нарушения целостности информации в базе данных.
2. НСД доступ к информации, вследствие которого может пострадать вся АС, в зависимости от цели нарушителя. Для этого будет выведена следующая модель нарушителя:

Таблица 3 – Модель нарушителя

|  |  |
| --- | --- |
| Пользователь | Модель нарушения |
| Инспектор отдела кадров | 1 уровень |
| Администратор | 4 уровень |
| Сотрудник | 1 уровень |

Таблица 4 – Справочные данные по моделям нарушителей:

|  |  |
| --- | --- |
| 1 уровень | Определяет самый низкий уровень возможности ведения диалога пользователя с АС- запуск задачи из фиксированного набора, реализация заранее предусмотренных функций по обработке информации. |
| 2 уровень | Определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации. |
| 3 уровень | Определяется возможностью управления функционирования АС, т.е. воздействие на базовое ПО системы и на состав и конфигурацию её оборудования. |
| 4 уровень | Определяется всем объёмом возможных лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации. |

Из полученных данных, известно, что некоторые пользователей в системе имеют доступ к конфиденциальной информации (служебная тайна и персональные данные), а один из них является администратором системы и оперирует ею, ему присваивает высоки уровень нарушителя.

Исходя из полученный данных и проведенного анализа, следует то, что системе следует присвоить класс защищенности «1Г».

Для реализации системы защиты в связи с выбранным классом защищенности будут реализованы следующие подсистемы: подсистема контроля доступа; подсистема регистрации и учета; подсистема целостности.

1. **ОПИСАНИЕ ПОСТАНОВКИ ЗАДАЧИ**

Система защиты для автоматизированной системы «Отдел кадров» разрабатывается для защиты персональных данных сотрудников и конфиденциальной информации предприятия. Поэтому появляется потребность в подсистемах разграничения доступа и контроля целостности информации в автоматизированной системе.

* 1. **Подсистема контроля доступа**

В подсистеме контроля доступа осуществляется идентификация и проверка подлинности субъектов при авторизации в системе по идентификатору и паролю.

Таблица 5 – Таблица кодов и паролей (ТКП)

|  |  |  |  |
| --- | --- | --- | --- |
| Логин | Пароль | ФИО | Должность |
| Belov1983 | \_4HU0OLEPI | Белов Александр Иванович | Инженер |
| Verger1324 | \_4HU0OPP73 | Енаров Петр Олегович | Инспектор отдела кадров |
| adminsys | \_4HU0MSPK6 | Долгов Андрей Николаевич | Администратор |

При регистрации нового сотрудника он сам записывает свой логин, который не будет совпадать с другими из базы данных. Пароль же генерируется автоматически и выдается администратором системы так же по необходимости меняется им же.

Таблица 6 – Возможности администратора

|  |  |
| --- | --- |
| ТКП | Просмотр/ редактирование |
| ТРП | Просмотр |
| Журнал учета | Просмотр |
| Целостность | Просмотр |
| Генерация пароля | Просмотр/ редактирование |
|  | Выход |

Таблица 7 – Возможности инспектора отдела кадров

|  |  |
| --- | --- |
| Сотрудники | Просмотр/редактирование |
| Табель | Просмотр/редактирование |
|  | Выход |

* 1. **Подсистема регистрации и учета**

Производится регистрация и учет событий в системе, а именно входа (выхода) субъектов в (из) системы. В параметрах регистрации в журнал событий указываются:

* дата и время входа (выхода) субъекта в (из) системы;
* результат авторизации: успешный, не успешный, несанкционированный доступ;
* а также записывается логин и пароль, которые вводились при входе в систему
* учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета с отметкой об их выдаче (приеме).

Таблица 8 – Журнал событий

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Логин | Пароль | Дата входа | Дата выхода | Статус |
| Belov1983 | \_4HU0OLEPI | 11/12/15 12:00 | 12/12/15 14:31 | Успешный вход |
| Verger1324 | trU0cOL123 | 12/12/15 11:12 |  | НСД |
| Verger1324 | trU0cOL123 | 12/12/15 12:13 |  | НСД |
| Verger1324 | ERU0cOL123 | 12/12/15 12:14 | 12/12/15 12:14 | Заблокирован |

* 1. **Подсистема целостности**
* Обеспечена целостность программных средств защиты информации несанкционированного доступа, обрабатываемой информации, а также неизменность программной среды.
* Обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
* Физическую охрану информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;
* Периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
* Наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Таблица 9 – Целостность информации

|  |  |  |
| --- | --- | --- |
| Перечень таблиц с конфиденциальной информацией | Контрольная сумма | Эталонная сумма |
| ТКП | 11310195 | 11310195 |
| ТРП | 427503 | 427503 |
| Сотрудники | 2483097 | 2483097 |

1. **. АНАЛИЗ МЕТОДОВ РЕШЕНИЯ**
   1. **Методы и средства защиты информации**

Защита данных в автоматизированной системе является основной задачей, так как в автоматизированной информационной системе походит работа с большими объемами данных, которые составляют конфиденциальные сведенья о персональных данных сотрудников и о самом коммерческом учреждении.

К основным методам защиты информации относятся следующие:

1. Ограничение доступа – заключается в создании физически замкнутой преграды вокруг объекта защиты.
2. Разграничение доступа – заключается в разделении информации, циркулирующей в системе и предоставлении доступа к ней лицам, в зависимости от их функциональных обязанностей и полномочий.
3. Разделение привилегий на доступ к информации – привилегия в системе, назначаются пользователями для разрешения или запрета выполнения различных действий в АИС.
4. Законодательные меры – положения, статьи. С 1 января 1997 года вступил в силу уголовный кодекс РФ, в котором содержится глава «Преступления в сфере компьютерной информации»: статьи 272 (неправомерный доступ КИ), 273 (создание, использование, распространение вредоносных программ), 274 (нарушение правил эксплуатации компьютера, компьютерных сетей и систем).

Современные методы защиты информации являются многоуровневыми и включают в себя:

1. Физические (создание физических препятствий в виде устройств и инженерных сооружений от проникновения нарушителя, также препятствие визуальному наблюдению, подслушиванию)
2. Аппаратные (Средства защиты процессов, памяти, устройств ввода-вывода, каналов связи, также включают устройства уничтожения информации, устройства сигнализации нарушения регистров границ памяти)
3. Программные (Средства защиты данных функционирующие в ПО, они выполняют функции защиты самостоятельно или в составе других средств защиты)
4. Организационные (технические и правовые мероприятия, осуществляющиеся в процессе создания и эксплуатации средств вычислительной техники для обеспечения безопасности данных)
5. Правовые (необходимость соблюдения юридических норм по обработки передаче информации)
6. Морально-этические (свод правил поведения сотрудников)

Учреждение, заинтересованное в сохранении и защите информации, непременно должно разработать политику безопасности, где будут отражены все меры и требования реализации. При реализации требований, отраженных в политике безопасности, зачастую используют программно-аппаратные способы защиты системы. Например, проведение аутентификации может осуществляться с помощью биометрических параметров человека, с использованием различных карт доступа, а также парольной защитой различ­ной степени сложности.

Анализируя требования ТЗ к постановке задачи необходимо обобщить и выделить ряд сходных задач, которые присутствуют практически в любой системе:

* ввод/вывод данных;
* обработка и соблюдение целостности;
* хранение;
* регистрация и учет событий;
* защита информации.

Реализация данных задач накладывает на разработчика определенные обязательства перед заказчиком, т.к. они должны быть выполнены строго в соответствии с ранее утвержденным ТЗ.

Для обеспечения защиты информации от НСД проводятся организационные мероприятия:

1. составляются должностные инструкции, в соответствии с которыми строится матрица разграничения полномочий (математическая модель системы защиты информации);
2. осуществляется физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
3. должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства;
4. должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление, и контроль работоспособности;
5. должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;
6. должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал;
7. учет защищаемых носителей должен проводиться в журнале с регистрацией их выдачи (приема);
8. должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации.
   1. **Средства вычислительной техники защиты от НСД к информации**

Настоящий Руководящий документ устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Устанавливается семь классов защищенности СВТ от НСД к информации. Самый низкий класс - седьмой, самый высокий - первый.

Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

* первая группа содержит только один седьмой класс;
* вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
* третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
* четвертая группа характеризуется верифицированной защитой и содержит только первый класс.

Выбор класса защищенности СВТ для автоматизированных систем, создаваемых на базе защищенных СВТ, зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

Применение в комплекте СВТ средств криптографической защиты информации по ГОСТ 28147-89 может быть использовано для повышения гарантий качества защиты.

Таблица 10 – Перечень показателей по классам защищенности СВТ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Наименование показателя | Класс защищенности | | | | | |
| 6 | 5 | 4 | 3 | 2 | 1 |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |
| Очистка памяти | - | + | + | + | = | = |
| Изоляция модулей | - | - | + | = | + | = |
| Маркировка документов | - | - | + | = | = | = |
| Защита ввода и вывода на отчуждаемый физический носитель информации | - | - | + | = | = | = |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |
| Идентификация и аутентификация | + | = | + | = | = | = |
| Гарантии проектирования | - | + | + | + | + | + |
| Регистрация | - | + | + | + | = | = |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |
| Надежное восстановление | - | - | - | + | = | = |
| Целостность КСЗ | - | + | + | + | = | = |
| Контроль модификации | - | - | - | - | + | = |
| Контроль дистрибуции | - | - | - | - | + | = |
| Гарантии архитектуры | - | - | - | - | - | + |
| Тестирование | + | + | + | + | + | + |
| Руководство для пользователя | + | = | = | = | = | = |
| Руководство по КСЗ | + | + | = | + | + | = |
| Тестовая документация | + | + | + | + | + | = |
| Конструкторская (проектная) документация | + | + | + | + | + | + |

* «-» - нет требований к данному классу;
* «+» - новые или дополнительные требования;
* «=» - требования совпадают с требованиями к СВТ предыдущего класса.
  1. **Обоснование выбора среды программирования**

Исходя из поставленной задачи и информационной модели, необходимо выбрать среду разработки системы. Существует много программных средств разработки подобных систем, каждая из них обладает определенными преимуществами и выполняет те или иные функции. Это такие приложения, как Microsoft Access, Visual C++, Visual Fox Pro.

Для разработки данной автоматизированной системы было выбрано приложение Visual Fox Pro.

Visual Fox Pro – это средство разработки баз данных. СУБД отличающееся производительностью и скоростью. Позволяет быстро и эффективно разрабатывать приложения, работающие с БД, как под управлением среды программирования, так и при помощи специального помощника конструктора wizard.

1. **. ИНФОРМАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ**
   1. **Концептуальная модель**

Концептуальная модель – это модель, представленная множеством понятий и связей между ними, определяющих смысловую структуру рассматриваемой предметной области или её конкретного объекта.

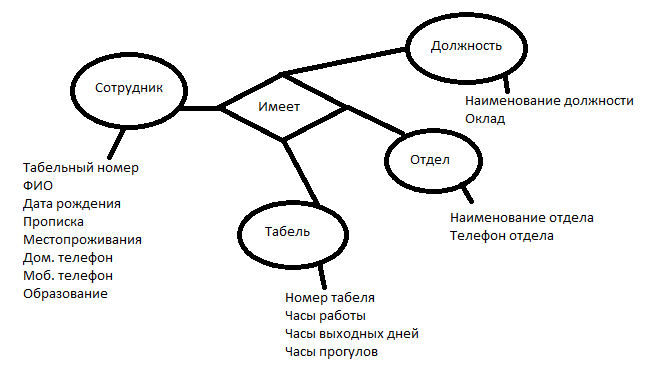


Рисунок 1 – Концептуальная модель

* 1. **Логическая модель**

Логическое проектирование — создание схемы базы данных на основе конкретной модели данных, например, реляционной модели данных. Для реляционной модели данных логическая модель — набор схем отношений, обычно с указанием первичных ключей, а также «связей» между отношениями, представляющих собой внешние ключи.

Логическая модель «Отдел Кадров» представлена на рисунке 2

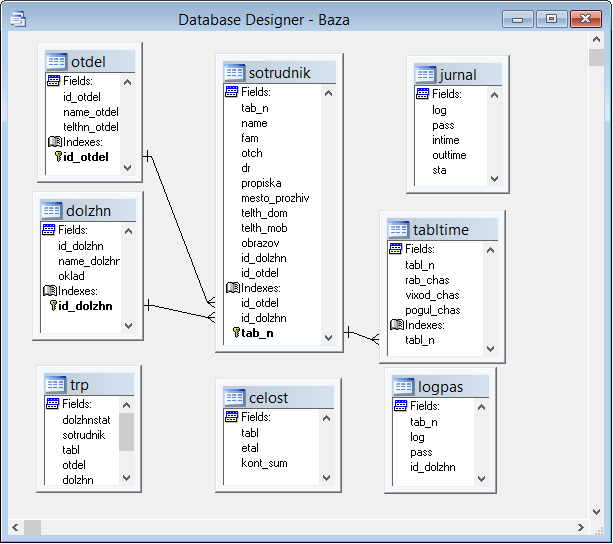


Рисунок 2 – Логическая модель

На рисунке 2 можно увидеть подсистему контроля доступа, которая реализована в таблицах jurnal (журнал учета) и logpass (ТКП). При попытке авторизации в системе будет проходит аутентификация (проверка совпадения пар логина и пароля в таблице logpass) при успешной аутентификации перед пользователем появится форма, к которой имеет доступ по таблице trp (ТРП) это реализация разграничения доступа. Если же пользователь не прошел аутентификации, то ему предоставляется еще 2 попытки, а при исчерпании попыток система блокируется.

* 1. **Физическая модель**

Физическая модель представляет собой совокупность БД на материальном носителе.



Рисунок 3 – Таблица отдела (otdel.dbf)

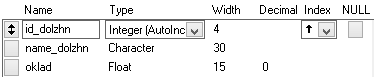


Рисунок 4 – Таблица должности (dolzhn.dbf)

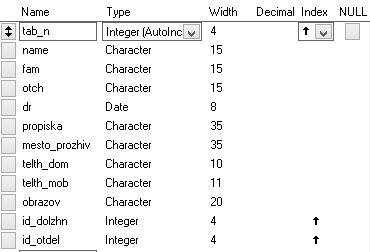


Рисунок 5 – Таблица сотрудников (sotrudnik.dbf)

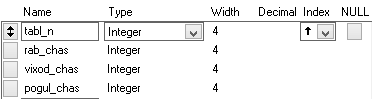


Рисунок 6 – Таблица табеля (tabltime.dbf)

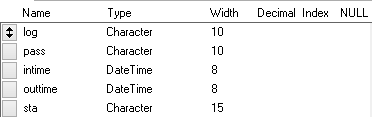


Рисунок 7 – Таблица журнала событий (jurnal.dbf)

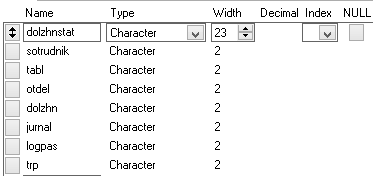


Рисунок 8 – Таблица ТРП (trp.dbf)

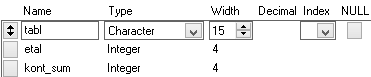


Рисунок 9 – Таблица целостности (celost.dbf)

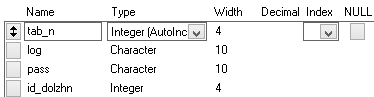


Рисунок 10 – Таблица ТКП (logpass.dbf)

1. **. РАЗРАБОТКА ПРОГРАММНО-ИНФОРМАЦИОННЫХ КОМПОНЕНТОВ СИСТЕМЫ**
   1. **Алгоритм программы**

Начало

Ввод логина и пароля

Регистрация входа

Аутентификация

Определение прав

REG++

Инспектор отдела кадров

Сотрудник

Администратор

(Администратор)

REG=3

Завершение работы

Неверный логин или пароль

Блокировка системы

Добавление сотрудника

ТКП

ТРП

Табель

ТРП

Журнал

Писк/модификация сотрудников

ТРП

Целостность

ТРП

Регистрация выхода

Конец

Рисунок 11 – Алгоритм авторизации

* 1. **Разработка пользовательского интерфейса**

****

Рисунок 12 – Пользовательский интерфейс

* 1. **Описание программных модуле**

Данная программная среда позволяет реализовать объектные модули объектно-ориентированного программирования, и это дает возможность реализовать множество различных программных модулей, которые были использовано в данном курсовом проекте.

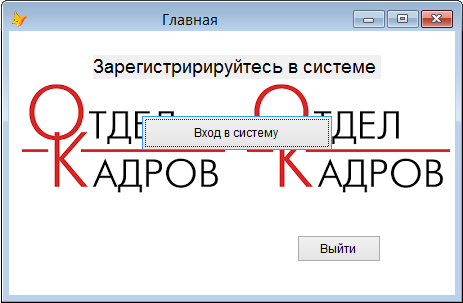


Рисунок 13 – Начальная форма

Обработчик кнопки «Вход в систему»

DO FORM login.scx

thisform.Release

Обработчик кнопки «Выход»

Quit

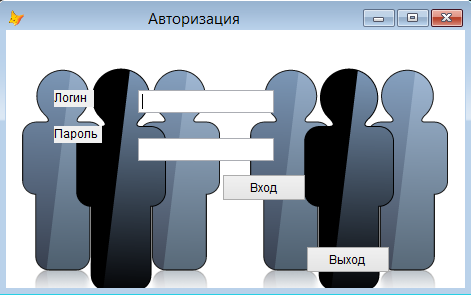


Рисунок 14 – Форма авторизации

Обработчик кнопки «Вход»

CLOSE TABLES

SET EXACT ON

IF EMPTY(thisform.Text1.value) OR EMPTY(thisform.Text2.value)

thisform.Refresh

MESSAGEBOX('Введите логин и пароль.',16,'Ошибка')

ELSE

USE logpas.dbf

LOCATE FOR ALLTRIM(log)=ALLTRIM(thisform.Text1.value) AND;

ALLTRIM(pass)=ALLTRIM(thisform.Text2.value)

IF FOUND()

USE jurnal.dbf

APPEND BLANK

replace jurnal.log WITH thisform.Text1.value

replace jurnal.pass WITH thisform.Text2.value

replace jurnal.intime WITH DATETIME()

replace jurnal.sta WITH 'Успешный вход'

USE logpas.dbf

LOCATE FOR ALLTRIM(log)=(ALLTRIM(thisform.Text1.value)) AND;

ALLTRIM(pass)=(ALLTRIM(thisform.Text2.value)) AND id\_dolzhn=3

IF FOUND()

DO FORM adm.scx

thisform.Release

ELSE

LOCATE FOR ALLTRIM(log)=ALLTRIM (thisform.Text1.value) AND;

ALLTRIM(pass)=ALLTRIM (thisform.Text2.value) AND id\_dolzhn=4

IF FOUND()

DO FORM bux.scx

thisform.Release

ELSE

DO FORM sotrud.scx

thisform.Release

ENDIF

ENDIF

reg = 0

ELSE

reg=reg+1

USE jurnal.dbf

IF reg = 3

APPEND BLANK

replace jurnal.log WITH thisform.Text1.value

replace jurnal.pass WITH thisform.Text2.value

replace jurnal.intime WITH DATETIME()

replace jurnal.sta WITH "Доступ заблокирован"

replace jurnal.outtime WITH DATETIME()

MESSAGEBOX('Система заблокирована!', 16)

thisform.Release

DO form blok.scx

else

APPEND BLANK

replace jurnal.log WITH thisform.Text1.value

replace jurnal.pass WITH thisform.Text2.value

replace jurnal.intime WITH DATETIME()

replace jurnal.sta WITH "Попытка входа"

MESSAGEBOX('Не верный логин или пароль. Повторите попытку.',16,'Ошибка')

ENDIF

ENDIF

ENDIF

Обработчик кнопки «Выход»

DO FORM nach.scx

thisform.Release

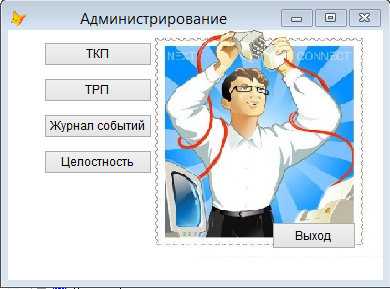


Рисунок 15 – Форма Администратора

Обработчик кнопки «ТКП»

DO FORM logpas.scx

thisform.Release

Обработчик кнопки «ТРП»

DO FORM trp.scx

thisform.Release

Обработчик кнопки «Журнал событий»

DO FORM jurnal.scx

thisform.Release

Обработчик кнопки «Целостность»

DO FORM celost.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

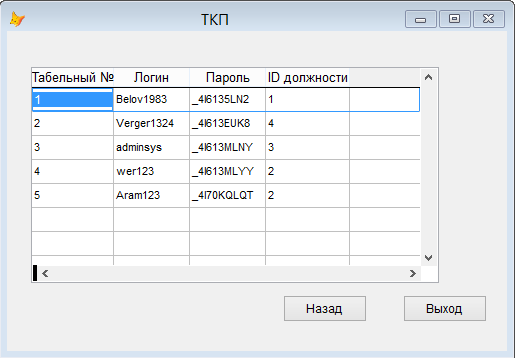


Рисунок 16 – Форма ТКП

Обработчик кнопки «Назад»

DO FORM adm.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

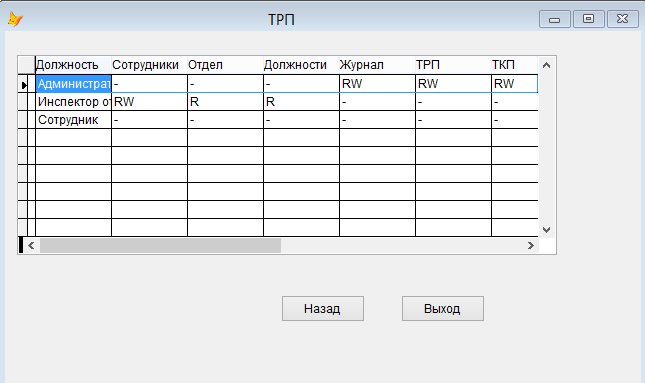


Рисунок 17 – Форма ТРП

Обработчик кнопки «Назад»

DO FORM adm.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO bottom

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

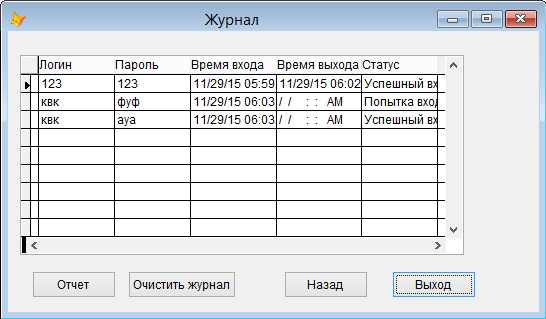


Рисунок 18 – Форма Журнала событий

Обработчик кнопки «Отчет»

REPORT FORM jurnal.frx NOWAIT TO PRINTER prompt

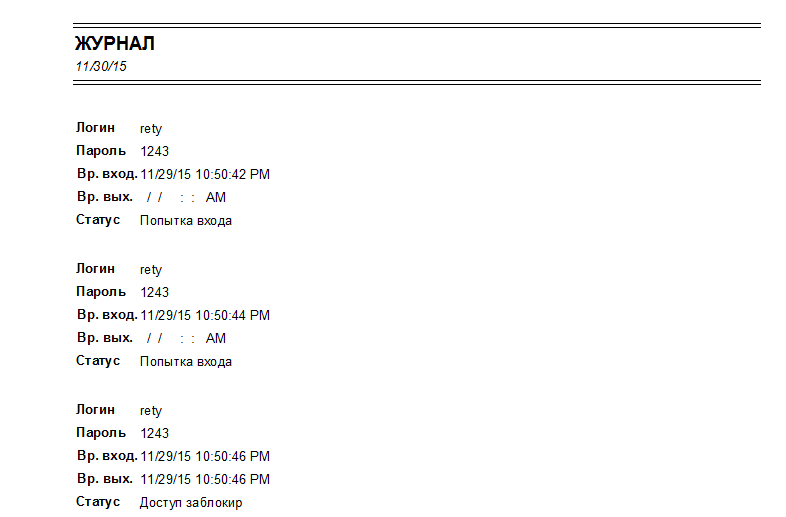


Рисунок 19 – Отчет по журналу событий

Обработчик кнопки «Отчистить Журнал»

USE jurnal.dbf

DELETE ALL

Pack

thisform.Release

DO FORM jurnal.scx

Обработчик кнопки «Назад»

DO FORM adm.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

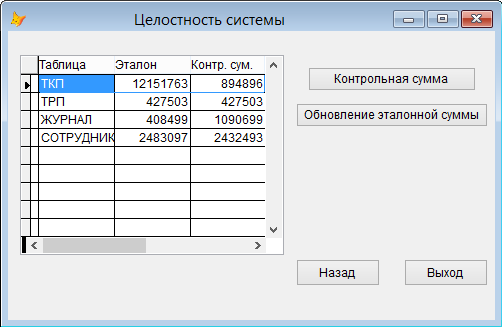


Рисунок 20 – Форма Целостности системы

Обработчик кнопки «Контрольная сумма»

CLOSE TABLES

USE logpas.dbf

t1=0

t2=0

t3=0

t4=0

FOR i=1 TO RECCOUNT()

GO i

s1=STR(logpas.tab\_n)

s2=logpas.log

s3=logpas.pass

s4=STR(logpas.id\_dolzhn)

t1=t1+VAL(SYS(2007,s1))

t2=t2+VAL(SYS(2007,s2))

t3=t3+VAL(SYS(2007,s3))

t4=t4+VAL(SYS(2007,s4))

ENDFOR

rez1=t1+t2+t3+t4

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='ТКП'

if FOUND()

replace kont\_sum WITH rez1

ENDIF

CLOSE TABLES

USE trp.dbf

t1=0

t2=0

t3=0

t4=0

t5=0

t6=0

t7=0

FOR i=1 TO RECCOUNT()

GO i

s1=trp.dolzhn

s2=trp.dolzhnstat

s3=trp.jurnal

s4=trp.logpas

s5=trp.otdel

s6=trp.sotrudnik

s7=trp.trp

t1=t1+VAL(SYS(2007,s1))

t2=t2+VAL(SYS(2007,s2))

t3=t3+VAL(SYS(2007,s3))

t4=t4+VAL(SYS(2007,s4))

t5=t5+VAL(SYS(2007,s5))

t6=t6+VAL(SYS(2007,s6))

t7=t7+VAL(SYS(2007,s7))

ENDFOR

rez2=t1+t2+t3+t4+t5+t6+t7

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='ТРП'

if FOUND()

replace kont\_sum WITH rez2

ENDIF

CLOSE TABLES

USE jurnal.dbf

t1=0

t2=0

t3=0

t4=0

t5=0

FOR i=1 TO RECCOUNT()

GO i

s1=DTOC(jurnal.intime)

s2=jurnal.log

s3=DTOC(jurnal.outtime)

s4=jurnal.pass

s5=jurnal.sta

t1=t1+VAL(SYS(2007,s1))

t2=t2+VAL(SYS(2007,s2))

t3=t3+VAL(SYS(2007,s3))

t4=t4+VAL(SYS(2007,s4))

t5=t5+VAL(SYS(2007,s5))

ENDFOR

rez3=t1+t2+t3+t4+t5

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='ЖУРНАЛ'

if FOUND()

replace kont\_sum WITH rez3

ENDIF

CLOSE TABLES

USE sotrudnik.dbf

t1=0

t2=0

t3=0

t4=0

t5=0

t6=0

t7=0

t8=0

t9=0

t10=0

t11=0

t12=0

FOR i=1 TO RECCOUNT()

GO i

s1=DTOC(sotrudnik.dr)

s2=sotrudnik.fam

s3=str(sotrudnik.id\_dolzhn)

s4=str(sotrudnik.id\_otdel)

s5=sotrudnik.mesto\_prozhiv

s6=sotrudnik.name

s7=sotrudnik.obrazov

s8=sotrudnik.otch

s9=sotrudnik.propiska

s10=str(sotrudnik.tab\_n)

s11=sotrudnik.telth\_dom

s12=sotrudnik.telth\_mob

t1=t1+VAL(SYS(2007,s1))

t2=t2+VAL(SYS(2007,s2))

t3=t3+VAL(SYS(2007,s3))

t4=t4+VAL(SYS(2007,s4))

t5=t5+VAL(SYS(2007,s5))

t6=t6+VAL(SYS(2007,s6))

t7=t7+VAL(SYS(2007,s7))

t8=t8+VAL(SYS(2007,s8))

t9=t9+VAL(SYS(2007,s9))

t10=t10+VAL(SYS(2007,s10))

t11=t11+VAL(SYS(2007,s11))

t12=t12+VAL(SYS(2007,s12))

ENDFOR

rez4=t1+t2+t3+t4+t5+t6+t7+t8+t9+t10+t11+t12

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='СОТРУДНИКИ'

if FOUND()

replace kont\_sum WITH rez4

ENDIF

CLOSE ALL

thisform.Release

DO FORM celost.scx

Обработчик кнопки «Обновление эталонной сумы»

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='ТКП'

if FOUND()

replace etal WITH kont\_sum

ENDIF

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='ТРП'

if FOUND()

replace etal WITH kont\_sum

ENDIF

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='ЖУРНАЛ'

if FOUND()

replace etal WITH kont\_sum

ENDIF

USE celost.dbf

LOCATE FOR ALLTRIM(tabl)='СОТРУДНИКИ'

if FOUND()

replace etal WITH kont\_sum

ENDIF

CLOSE ALL

thisform.Release

DO FORM celost.scx

Обработчик кнопки «Назад»

DO FORM adm.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

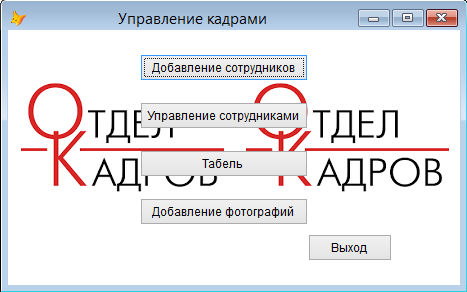


Рисунок 21 – Форма управления кадрами

Обработчик кнопки «Добавление сотрудников»

DO FORM addsotrudnik.scx

thisform.Release

Обработчик кнопки «Управление сотрудниками»

DO FORM sotr.scx

thisform.Release

Обработчик кнопки «Табель»

DO FORM tabl.scx

thisform.Release

Обработчик кнопки «Добавление фотографий»

DO FORM foto.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

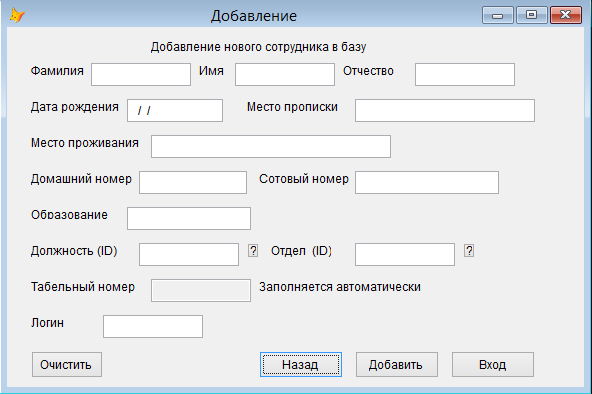


Рисунок 22 – Форма добавления сотрудниками

Обработчик кнопки «Назад»

DO FORM bux.scx

thisform.Release

Обработчик кнопки «Добавить»

CLOSE TABLES

IF EMPTY(thisform.Text1.value) or EMPTY(thisform.Text2.value) OR EMPTY(thisform.Text3.value) OR EMPTY(thisform.Text4.value) or;

EMPTY(thisform.Text5.value) OR EMPTY(thisform.Text6.value) OR EMPTY(thisform.Text7.value) OR EMPTY(thisform.Text8.value) or;

EMPTY(thisform.Text9.value)OR EMPTY(thisform.Text11.value) OR EMPTY(thisform.text12.value) OR EMPTY(thisform.text13.value)

thisform.Refresh

MESSAGEBOX('Введены не все данные.',16,'Ошибка')

else

USE logpas.dbf

APPEND BLANK

replace id\_dolzhn WITH val(thisform.text12.value)

replace log WITH thisform.text11.value

REPLACE pass WITH SYS(2015)

USE sotrudnik.dbf

APPEND BLANK

replace fam WITH thisform.text1.value

replace name WITH thisform.text2.value

replace otch WITH thisform.text3.value

replace dr WITH thisform.text4.value

replace propiska WITH thisform.text5.value

replace mesto\_prozhiv WITH thisform.text6.value

replace telth\_dom WITH thisform.text7.value

replace telth\_mob WITH thisform.text8.Value

replace obrazov WITH thisform.text9.value

replace id\_dolzhn WITH val(thisform.text12.value)

replace id\_otdel WITH val(thisform.text13.value)

thisform.text10.value=tab\_n

MESSAGEBOX('Сотрудник добавлен')

endif

Обработчик кнопки «Очистить»

CLOSE ALL

thisform.Release

DO FORM addsotrudnik.scx

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

Обработчик кнопки «?(1)»

select id\_dolzhn,name\_dolzhn from dolzhn

Обработчик кнопки «?(2)»

select id\_otdel,name\_otdel from otdel

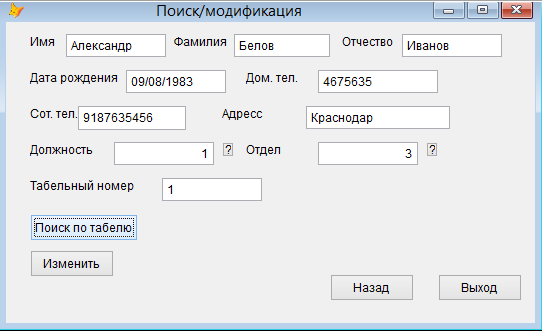


Рисунок 23 – Форма управления сотрудниками

Обработчик кнопки «Поиск по табелю»

CLOSE TABLES

USE sotrudnik.dbf

IF LEN(ALLTRIM(thisform.text10.value))=0

MESSAGEBOX('вы не ввели критерий поиска',0,'сообшение')

ELSE

GO TOP

LOCATE FOR tab\_n=VAL(ALLTRIM(thisform.text10.value))

IF FOUND()=.t.

thisform.text1.Value=name

thisform.text2.Value=fam

thisform.text3.Value=otch

thisform.text4.Value=dr

thisform.text5.Value=telth\_dom

thisform.text6.Value=telth\_mob

thisform.text7.Value=mesto\_prozhiv

thisform.text8.Value=id\_dolzhn

thisform.text9.Value=id\_otdel

USE dolzhn.dbf

ELSE

MESSAGEBOX('запись не найдена',0,'сообщение')

ENDIF

ENDIF

Обработчик кнопки «Изменить»

CLOSE TABLES

IF EMPTY(thisform.text1.Value) OR EMPTY(thisform.text2.Value) OR EMPTY(thisform.text3.Value) OR;

EMPTY(thisform.text4.Value) OR EMPTY(thisform.text5.Value) OR EMPTY(thisform.text6.Value) OR;

EMPTY(thisform.text7.Value) OR EMPTY(thisform.text8.Value) OR EMPTY(thisform.text9.Value) OR EMPTY(thisform.text10.Value)

MESSAGEBOX('Вы ввели не все данные',0,'сообшение')

else

USE sotrudnik.dbf

LOCATE FOR tab\_n=val(ALLTRIM(thisform.text10.value))

IF FOUND()

replace name WITH thisform.text1.Value

replace fam WITH thisform.text2.Value

replace otch WITH thisform.text3.Value

replace dr WITH thisform.text4.Value

replace telth\_dom WITH thisform.text5.Value

replace telth\_mob WITH thisform.text6.Value

replace mesto\_prozhiv WITH thisform.text7.Value

replace id\_dolzhn WITH thisform.text8.Value

replace id\_otdel WITH thisform.text9.Value

MESSAGEBOX('Запись изменена',0,'сообщение')

ELSE

MESSAGEBOX('Табель не найден',0,'сообщение')

ENDIF

ENDIF

Обработчик кнопки «Назад»

USE bux.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

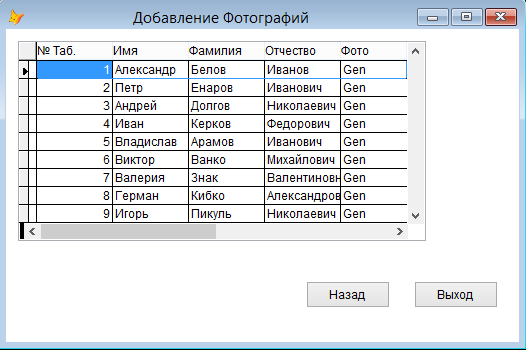


Рисунок 24 – Форма добавления фотографий

Обработчик кнопки «Назад»

USE bux.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

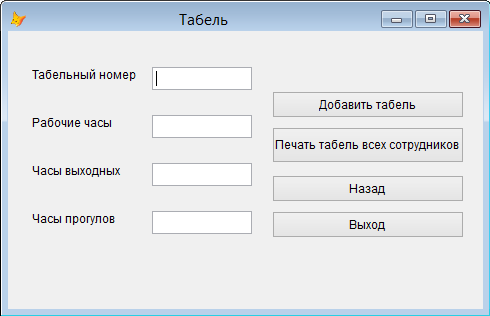


Рисунок 25 – Форма табель

Обработчик кнопки «Добавить табель»

IF EMPTY(thisform.text1.value) OR EMPTY(thisform.text2.value) OR EMPTY(thisform.text3.value) OR EMPTY(thisform.text4.value)

MESSAGEBOX('Введены не все данные',16)

else

USE tabltime.dbf

APPEND BLANK

replace tabl\_n WITH val(thisform.text1.value)

replace rab\_chas WITH val(thisform.text2.value)

replace vixod\_chas WITH val(thisform.text3.value)

replace pogul\_chas WITH val(thisform.text4.value)

MESSAGEBOX('Табель добавлен')

thisform.Refresh

thisform.text1.value=''

thisform.text2.value=''

thisform.text3.value=''

thisform.text4.value=''

endif

Обработчик кнопки «Печать табель всех сотрудников»

REPORT FORM tabl.frx NOWAIT TO PRINTER prompt

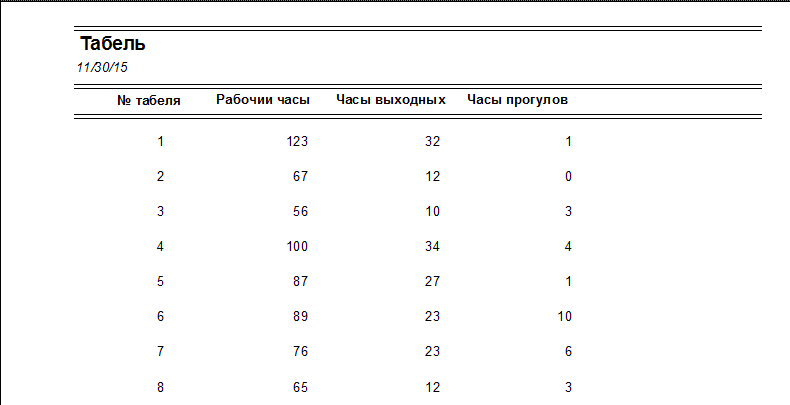


Рисунок 26 – Отчет по табелю

Обработчик кнопки «Назад»

DO FORM bux.scx

thisform.Release

Обработчик кнопки «Выход»

USE jurnal.dbf

GO BOTTOM

replace outtime WITH DATETIME()

DO FORM nach.scx

thisform.Release

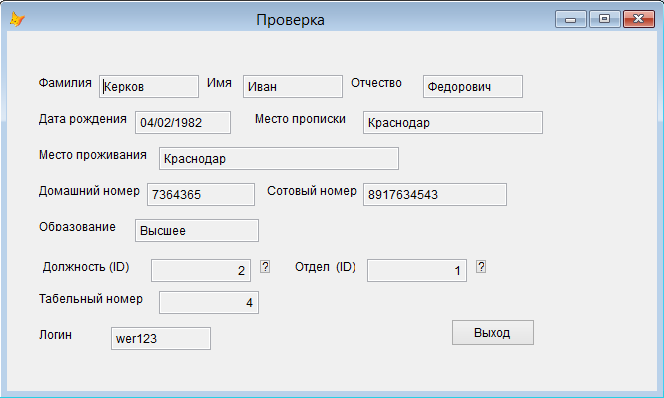


Рисунок 27 – Форма сотрудника

Код формы

CLOSE TABLES

USE jurnal.dbf

GO bottom

t1=jurnal.log

thisform.text11.Value=t1

USE logpas.dbf

LOCATE FOR alltrim(log)=t1

IF FOUND()

t2=logpas.tab\_n

thisform.text10.Value=t2

USE sotrudnik.dbf

LOCATE FOR tab\_n=t2

IF FOUND()

thisform.text1.Value=fam

thisform.text2.Value=name

thisform.text3.Value=otch

thisform.text4.Value=dr

thisform.text5.Value=propiska

thisform.text6.Value=mesto\_prozhiv

thisform.text7.Value=telth\_dom

thisform.text8.Value=telth\_mob

thisform.text9.Value=obrazov

thisform.text12.Value=id\_dolzhn

thisform.text13.Value=id\_otdel

ENDIF

ENDIF

* 1. **Тестирование подсистем АИС**
     1. **Тестирование подсистемы управления доступом**

Для проверки управления доступом в форме авторизации рисунок 14 допустим 3 ошибки при вводе логина и пароля. После чего произойдет переход на форму блокировки.

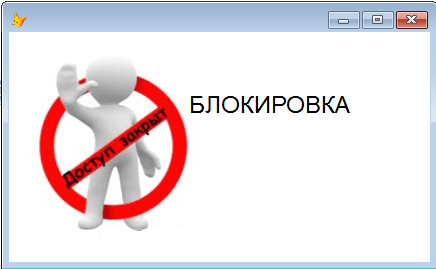


Рисунок 28 – Форма блокировки

* + 1. **Тестирование подсистемы регистрации и учета**

После проведенной ранние блокировки авторизуемся под верным логином и паролем. После всех этих попыток авторизоваться, в журнале регистрации событий уже внесены все наши попытки авторизации.

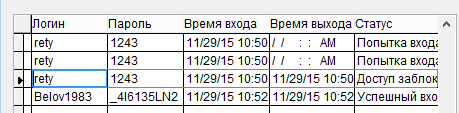


Рисунок 29 – Журнал регистрации событий

1. **. ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ**
   1. **Инструкция для администратора**

Регистрация. После запуска приложения необходимо безошибочно ввести свои регистрационные данные (логин и пароль). При вводе данных необходимо учесть язык ввода и делать различия между прописными и печатными буквами. После ввода данных нажать кнопку «ВХОД».

Если пользователь, вошедший в программу, не является администратором, то перед ним появится экранная форма в соответствии с должностными обязанностями.

Если пользователь, зарегистрировавшийся в программе, является администратором, то перед ним появится экранная форма, которая содержит:

Журнал. Просмотр журналов регистрации пользователей и событий.

ТРП. Просмотр и назначение прав пользователям.

Генерация пароля. Данная форма предназначена для генерации случайного пароля сотрудникам.

Целостность. Предоставляет возможность считать контрольную сумму всех таблиц, таблицы кодов паролей, таблицы разграничения прав, а также пересчитывать эталонную и контрольную суммы.

Таблица кодов паролей. Предоставляет возможность смены пароля для уже существующего пользователя.

При возникновении нестандартной ситуации необходимо вызвать администратора системы.

* 1. **Инструкция для пользователей**

Данная система предназначена для добавления данных о сотрудниках, редактирования их персональных данных. Также каждому из сотрудников (инженер, бухгалтер, оператор и т.д.) предоставляется возможность просматривать и проверять правильность личных персональных данных.

* + 1. **Техника безопасности**

Требования техники безопасности перед началом работы.

Перед началом работы пользователю необходимо:

* осмотреть рабочее место, убедиться в том, чтобы на нём не было посторонних предметов, которые могут помешать работе;
* отрегулировать освещенность рабочего места, и уровень спинки стула, для комфортной работы;
* проверить наличие вспомогательной техники: принтер, сканер.
  + 1. **Требование безопасности во время работы**

Во время работы пользователь обязан:

* заниматься только порученной ему работой;
* следить за чистотой и проветриванием помещения;
* следить за порядком на рабочем месте;
* соблюдать правила эксплуатации при работе с вычислительной и оргтехникой.
* соблюдать санитарные нормы;
* соблюдать режимы работы и отдыха.

Пользователю во время работы запрещается:

* подключать к компьютеру носители информации, не проверенные на наличие вирусов;
* при поломке компьютера пытаться его самостоятельно починить;
* самостоятельно удалять/устанавливать программное обеспечение с компьютера;
* ставить посторонние предметы на системный блок, монитор, рабочее место;
* самостоятельно извлекать из принтера непригодную бумагу;
* открывать системный блок.
  + 1. **Требование безопасности в аварийных ситуациях**

Пользователь обязан:

* в случае обнаружения повреждения электрооборудования немедленно отключить питание и сообщить администратору;
* при любых сбоях в работе технического оборудования или программных средств немедленно вызвать представитель инженерно-технической службы эксплуатации вычислительной техники.
* ежемесячно проверять локальные диски компьютера на наличие вирусов;
* при возгорании оборудования, отключить электропитание и принять меры к тушению пожара, вызвать пожарную команду, оповестить о происшествии руководителя.
  + 1. **Требование к безопасности после окончания работы**

Пользователь обязан:

* произвести корректное завершение всех активных приложений;
* выключить питание системного блока;
* отключить питание всех вспомогательных периферийных устройств;
* отключить блок питания;
* осмотреть и привести в порядок рабочее место;

1. **ЗАКЛЮЧЕНИЕ**

В процессе реализации курсового проекта была достигнута цель – разработки защищенной АС «Отдел кадров» для автоматизации учета сотрудников предприятия и обеспечения основных подсистем безопасности: разграничения доступа, регистрации и учета, и обеспечения информационной целостности системы.

Данная система отвечает поставленным целям: простой пользовательский интерфейс, отчет документации, функции добавления, редактирования, удаления и поиска необходимых данных, защита от НСД.

Процесс создания системы производится согласно разделам пояснительной записки: были проанализированы и изучены поставленные цели: проанализирована предметная область, выполнена постановка задачи и концептуальное проектирование, разработана технологическая цепочка обработки информации, были обоснованы выбранные методы решения создания АС «Отдел кадров», построены логическая и физическая модели данных, создание программно-информационного компонента.

**Список используемых источников**

* + 1. Лебедев А.Н. FoxPro 9.0 Самоучитель.
    2. Гурвиц Г.А. Разработка реального приложения с использованием Microsoft Visual FoxPro 9
    3. ГОСТ Р 50922-2006. Национальный стандарт РФ. Защита информации. Основные термины и определения.
    4. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
    5. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
    6. Постановление от 1 ноября 2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
    7. Приказ Федеральной службы по техническому и экспортному контролю № 21 от 14.05.2013 г. "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
    8. Руководящий документ Гостехкомиссии России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации / Гостехкомиссия России. - М., 1992

**Техническое задание**

1. **Требования к системе.**
   1. Требования к системе в целом.
      1. Автоматизированное рабочее место (АРМ) должно функционировать на рабочей станции сотрудника предприятия.
      2. Работать с АРМ будет инспектора отдела кадров и сотрудники предприятия, которые должны иметь начальные навыки работы с персональным компьютером с ОС семейства Windows. Перед использованием АРМ, инспектора отдела кадров и сотрудники предприятия должны пройти инструктаж и усвоить основные правила работы с системой.
      3. Настройка системы должна производиться администратором, имеющим среднее специальное или высшее техническое образование.
      4. Ежемесячно необходимо проверять ОС ТТК, на котором эксплуатируется АРМ, на наличие вредоносного ПО, проводить дефрагментацию жесткого диска и проверку свободного дискового пространства.
      5. АРМ должна функционировать в течение рабочего дня инспектора отдела кадров и сотрудника предприятия
      6. АРМ должна включать в себя подсистему справки. Интерфейс АРМ не должен вызывать у пользователя работающего с ним, двусмысленного понимания назначения какого-либо компонента.
      7. Необходимо внедрить в АРМ подсистему защиты информации, которая позволит ограничивать доступ к системе пользователям, не имеющим право работать с АРМ.
      8. Система должна быть устойчива к появлению аварийных ситуаций технического компонента АРМ, т.е в случае нарушения работоспособности ОС ПК, АРМ и используемая база данных не должны быть повреждена.
      9. Обслуживающий персонал должен организовать систему бесперебойного питания для технического компонента АРМ.
      10. АРМ может эксплуатироваться только на территории РФ, при этом авторские права не должны быть нарушены.
   2. Требования к функциям и задачам системы.

Подсистема защиты АС должна реализовать следующие задачи:

* + 1. Идентификация и аутентификация пользователей при входе в АИС (ввод логина и пароля в регистрационном окне при входе в систему).
    2. Предоставление пользователю права доступа к данным АИС (в зависимости от занимаемой должности сотрудник имеет доступ только к той БД и информации, на которые ему назначены права).
    3. Обеспечение целостности данных (проверка таблиц системы на измененной хранимой в них информации, в целях выявления НСД к информации).
    4. Разграничение полномочий пользователей (каждый пользователь имеет определенный набор прав доступа к информации, содержащейся в АС).
  1. Требования к видам обеспечения
     1. Программный компонент АРМ должен работать в ОС семейства Windows, а именно: WindowsХР SP2 и выше, WindowsVista SP1 и выше, Windows 7 SP1 и выше.
     2. АРМ использует систему управления базами данных(СУБД) - VisualFoxPro 9.0;
     3. Для стабильной работы АРМ, технический компонент должен содержать следующие характеристики.
        1. Видеокарта с объемом памяти не менее 512 Мб;
        2. Дисплей с разрешением не менее 1024x768;
        3. ЦП с тактовой частотой не менее 2,5 ГГц;
        4. ОЗУ с объемом памяти не менее 1 Гб;
        5. Объем жесткого диска не менее 8 Гб;
        6. ИБП;
        7. Принтер для печати отчетов;
        8. ОС семейства WindowsХР SP2 и выше;
        9. Антивирусный продукт с постоянным обновлением;